Computation of the Galois groups
occurring in M. Papanikolas's study of Carlitz logarithms

Charlotte Hardouin (IWR, Heidelberg)

February 23, 2007

1 Introduction

In this note, we give an alternative presentation of one of the ingredients occurring in M. Papanikolas's proof of the algebraic independence of Carlitz logarithms [7]. More precisely, the main theorem of [7] reduces the problem to the computation of the Galois group G_X of a certain t-motive X, and we present an alternative proof of the computation of G_X. The method is inspired from [5], and should apply to other situations, such as logarithms of Drinfeld elliptic modules, or values of ζ-functions. We now recall the statement of Papanikolas's theorem, and the notations of his article, which will be kept throughout this note.

1.1 Notations

Let $\mathbb{F}_q$ the field of q-elements, where q is a prime power of p. Let $k = \mathbb{F}_q(\theta)$, where θ is transcendental over $\mathbb{F}_q$, and define an absolute valuation $|.|_\infty$ at the infinite place of k such that $|\theta|_\infty = q$. let k_∞ be the ∞-adic completion of k, let $\overline{k_\infty}$ be an algebraic closure, let $\mathbb{K}$ be the ∞-adic completion of $\overline{k_\infty}$, $\mathbb{T} := \mathbb{K}\{t\}$ is the ring of restricted power series and let $\overline{k}$ be the algebraic closure of k in $\mathbb{K}$. For $f = \sum_i a_i t^i$ in $\mathbb{T}$, we set $f^{(-1)} = \sum_i a_i^q t^i$.

Definition 1.1 (see [7]) *We let $\mathcal{T}$ be the category of t-motives in the sense of [7], 3.4.10.*

We recall that $\mathcal{T}$ is a strictly full Tannakian sub-category of the category $\mathcal{R}$ of rigid analytically trivial pre-t-motives. Objects in $\mathcal{R}$ correspond to certain σ-difference equations over $\overline{k}(t)$, and a fiber functor ω on $\mathcal{T}$ is provided by rigid analytic trivialization. In particular, $\mathcal{T}$ is a neutral tannakian category over $\mathbb{F}_q(t)$. We denote its identity object by $\mathbf{1}$, and for any X in $\mathcal{T}$, we write $G_X = Aut^\otimes(\omega_{|<X>})$ for the Galois group of X attached to the fiber functor ω, see [7], 3.5.2, 4.4.1 and 5.4.10. By [7], 5.2.12.b, this is a reduced affine group scheme over $\mathbb{F}_q(t)$.

1.2 Exemples of σ-equations associated to objects of $\mathcal{T}$

1. **The Carlitz motive**

We define the Carlitz motive to be the pre-t-motive $\mathcal{C}$ whose underlying $\overline{k}(t)$-vector space is $\overline{k}(t)$ itself and on which σ acts by

$$\sigma(f) := (t - \theta)f^{(-1)}, f \in \mathcal{C}$$

(a) The Carlitz motive is rigid analytically trivial and one of its analytic trivialization is given by the function $\frac{1}{\Omega}$ (see [7] 3.3.5).

(b) The number $\tilde{\pi} = -\frac{1}{\Omega(\theta)}$ is the *Carlitz period*.

(c) The Galois group $G_{\mathcal{C}}$ of $\mathcal{C}$ is equal to $\mathbb{G}_m$.

(d) Moreover, we have $End_{\mathcal{T}}(C, C) = \mathbb{F}_q(t)$ (cf. [7] 3.5.3).

2. **The Carlitz logarithm motive**

Let $\alpha_i \in \overline{k}^*$ with $|\alpha_i|_\infty < |\theta|_\infty^{q/(q-1)}$. Set :

$$\Phi(\alpha_i) := \begin{pmatrix} (t - \theta) & 0 \\ \alpha_i^{(-1)}(t - \theta) & 1 \end{pmatrix}.$$

$\Phi(\alpha_i)$ defines a pre-t-motive $X(\alpha_i)$, which is an extension in the category $\mathcal{T}$ of $\mathbf{1}$ by the Carlitz motive $\mathcal{C}$

$$0 \longrightarrow \mathcal{C} \longrightarrow X(\alpha_i) \longrightarrow \mathbf{1} \longrightarrow 0 \ .$$

Indeed, the pre-t-motive $X(\alpha_i)$ is rigid analytically trivial (see [7] prop. 7.1.3) and its trivialization is given by :

$$\Psi(\alpha_i) := \begin{pmatrix} \Omega & 0 \\ \Omega L_{\alpha_i} & 1 \end{pmatrix},$$

where the function L_{α_i} is defined as in [7], 7.1.1 : this is an element of $\mathbb{T}$ satisfying the functional equation :

$$\sigma(L_{\alpha_i}) = \alpha_i^{(-1)} + \frac{L_{\alpha_i}}{(t - \theta)},$$

whose value at $t = \theta$ is equal to the Carlitz logarithm $Log_{\mathcal{C}}(\alpha_i)$ of α_i.

3. **The multiple Carlitz logarithm motive**

Let $\alpha_1, ..., \alpha_r \in \overline{k}^*$ with $|\alpha_i|_\infty < |\theta|_\infty^{q/(q-1)}$. Set :

$$\Phi(\alpha_1, ..., \alpha_r) := \begin{pmatrix} t - \theta & 0 & \cdots & 0 \\ \alpha_1^{(-1)}(t - \theta) & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_r^{(-1)}(t - \theta) & 0 & \cdots & 1 \end{pmatrix}.$$

$\Phi(\alpha_1, ..., \alpha_r)$ defines a pre-t-motive $X(\alpha_1, ..., \alpha_r)$ which is an extension of $\mathbf{1}^r$ by the Carlitz motive $\mathcal{C}$:

$$0 \longrightarrow \mathcal{C} \longrightarrow X(\alpha_1, ..., \alpha_r) \longrightarrow \mathbf{1}^r \longrightarrow 0 \ .$$

The pre-t-motive $X(\alpha_1, ..., \alpha_r)$ is rigid analytically trivial (see [7] prop. 7.1.3) and its trivialization is given by :

$$\Psi(\alpha_1, ..., \alpha_r) := \begin{pmatrix} \Omega & 0 & \cdots & 0 \\ \Omega L_{\alpha_1} 1 & \cdots & & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \Omega L_{\alpha_r} & 0 & \cdots & 1 \end{pmatrix}.$$

As in [5], proof of Cor. 2.2, we have :

Lemma 1.2 *The tannakian category generated by $X(\alpha_1, ..., \alpha_r)$ in $\mathcal{T}$ is equal to the Tannakian category generated by the motive $\bigoplus_{i=1}^r X(\alpha_i)$.*

1.3   Papanikolas's theorems on algebraic independence.

Theorem 1.3 (Theorem 7.4.2 in [7]) *Let $\lambda_1, ..., \lambda_r \in \mathbb{K}$ satisfy $exp_C(\lambda_i) \in \overline{k}$ for $i = 1, ..., r$. If $\lambda_1, ..., \lambda_r$ are linearly independent over k, then they are algebraically independent over $\overline{k}$.*

Since the period $\tilde{\pi}$ satisfies $exp_{\mathcal{C}}(\tilde{\pi}) = 0$, we can rephrase Theorem 1.3 as follow : Let $\lambda_1, ..., \lambda_r \in \mathbb{K}$ satisfy $exp_C(\lambda_i) \in \overline{k}$ for $i = 1, ..., r$. If $\lambda_1, ..., \lambda_r, \tilde{\pi}$ are linearly independent over k, then they are algebraically independent over $\overline{k}$.

Because the indetermination of the Carlitz logarithm is given by k-multiples of $\tilde{\pi}$ (cf. [7], 7.4.1), this is in turn equivalent to

Theorem 1.4 *Let $\alpha_1, ..., \alpha_r \in \overline{k}^*$ with $|\alpha_i|_\infty < |\theta|_\infty^{q/(q-1)}$. Assume that $\tilde{\pi}, log_{\mathcal{C}}(\alpha_1), ..., log_{\mathcal{C}}(\alpha_r)$ are linearly independent over k. Then they are algebraically independent over $\overline{k}$.*

Now, $\tilde{\pi} = -\frac{1}{\Omega(\theta)}, log_{\mathcal{C}}(\alpha_1) = L_{\alpha_1}(\theta), ..., log_{\mathcal{C}}(\alpha_r) = L_{\alpha_r}(\theta)$. Combining the main Theorem 1.1.7 of his article together with a previous transcendence criterion (Theorem 6.1.1), Papanikolas reduces the proof of Theorem 1.4 to showing :

Theorem 1.5 (Theorem 7.3.2.c in [7]) *Let $\alpha_1, ..., \alpha_r \in \overline{k}^*$ with $|\alpha_i|_\infty < |\theta|_\infty^{q/(q-1)}$. Assume that $\tilde{\pi}, log_{\mathcal{C}}(\alpha_1), ..., log_{\mathcal{C}}(\alpha_r)$ are linearly independent over k. Then the dimension of the Galois group G_X of the t-motive $X = X(\alpha_1, ..., \alpha_r)$ is equal to $r + 1$.*

1.4 Sketch of the proof of Theorem 1.5

Following [7], we will work in the framework of the Tannakian category $\mathcal{T}$ of t-motives, cf. Definition 1.1. As just recalled, the method of M. Papanikolas for proving Theorem 1.3 is to compute the Galois group G_X of the t-motive X. This is the content of Theorem 7.3.2 of [7], where G_X is denoted by Γ_X. Note, however, that the paragraph following (7.2.4.1) needs some clarification, since Γ_X is not a linear subspace. In this note, we will give a tannakian version of the computation of G_X, which while settling this point, actually simplifies the proof of [7], and points towards further generalizations of Theorem 1.3.

So, we have to compute the dimension of the Galois group attached to the motive $X = X(\alpha_1, ..., \alpha_r)$. To this purpose, we deduce from Lemma 1.2 that the Galois group of X is equal to the Galois group G of $\bigoplus_{i=1}^{r} X(\alpha_i)$. As in [7], 7.2.2, we see that the quotient of G by its unipotent radical is isomorphic to the Galois group of the Carlitz motive $\mathcal{C}$, i.e to $\mathbb{G}_m$. Therefore, it remains to compute the dimension of the unipotent radical of G, that is the unipotent radical of the Galois group of a sum of extensions of $\mathbf{1}$ by the Carlitz motive.

To compute the latter dimension, we will use the theorems of Section 2 below, which reduce the problem to a question of linear algebra ; this section combines the arguments of [5] with Papanikolas's crucial observation that the unipotent radical is a *vectorial* group, see [7], 7.2.3. Finally, Section 3 completes the proof of Theorem 1.5, along the lines of [7], bottom of p. 50.

2 Computation of Galois groups in Tannakian categories in characteristic p

Let p be a prime number. Let $(\mathbf{T}, \omega)$ be a neutral Tannakian category over a field C of characteristic p. Let $\mathbf{1}$ denotes the unit object of $\mathbf{T}$, so that $C = End(\mathbf{1})$ and $\omega : \mathbf{T} \mapsto Vect_C$. In the application to [7], $\mathbf{T} = \mathcal{T}$ and $C = \mathbb{F}_q(t)$, where q is a power of p and t is transcendental over $\mathbb{F}_q$.

For any object $\mathcal{X}$ in $\mathbf{T}$, we denote by $G_{\mathcal{X}}$ the linear algebraic group scheme $Aut^{\otimes}(\omega|_{<\mathcal{X}>})$ over C. Furthermore, we identify C-vector spaces such as $\omega(\mathcal{X})$ to *vectorial groups* over C.

Theorem 2.1 *Let $\mathcal{Y}$ be an object of $\mathbf{T}$, and let $\mathcal{U}$ be an extension of $\mathbf{1}$ by $\mathcal{Y}$. Assume that $G_{\mathcal{U}}$ is reduced, that $G_{\mathcal{Y}} = \mathbf{G}_m$, and that the action of $\mathbf{G}_m$ on $\omega(\mathcal{Y})$ is given by its canonical character. Then the unipotent radical of the Galois group $G_{\mathcal{U}}$ is equal to $\omega(\mathcal{V})$ where $\mathcal{V}$ is the smallest sub-object of $\mathcal{Y}$ such that $\mathcal{U}/\mathcal{V}$ is a trivial extension of $\mathbf{1}$ by $\mathcal{Y}/\mathcal{V}$.*

Proof
First of all, we remark that every $\mathbf{G}_m$-module of finite dimension over C is completely reducible (see [6] p.35). By Tannaka theorem (see [4]) , there is an equivalence of category

4

between $< \mathcal{Y} >$ and the category $Rep_{G_\mathcal{Y}}$ of $G_\mathcal{Y}$-modules of finite dimension over C. Then, it is clear that $\mathcal{Y}$ is a completely reducible object in $\mathbf{T}$.

Existence of the smallest sub-object

Let us denote by $\mathbf{V}$ the set of sub-objects $\mathcal{W}$ of $\mathcal{Y}$ such that $\mathcal{U}/\mathcal{W}$ is a trivial extension of $\mathbf{1}$ by $\mathcal{Y}/\mathcal{W}$. It is enough to prove that if $\mathcal{V}_1$ and $\mathcal{V}_2$ are in $\mathbf{V}$, their intersection $\mathcal{W}$ lies in $\mathbf{V}$.

Because $\mathcal{Y}$ is completely reducible, there exist three sub-objects $\mathcal{V}'$, $\mathcal{W}'_1$, $\mathcal{W}'_2$ of $\mathcal{Y}$ such that :
1. $\mathcal{V}_1 = \mathcal{W} \oplus \mathcal{W}'_1$, $\mathcal{V}_2 = \mathcal{W} \oplus \mathcal{W}'_2$.
2. $\mathcal{Y} = \mathcal{V}_1 \oplus \mathcal{W}'_2 \oplus \mathcal{V}' = \mathcal{V}_2 \oplus \mathcal{W}'_1 \oplus \mathcal{V}' = \mathcal{W} \oplus \mathcal{W}'_2 \oplus \mathcal{W}'_1 \oplus \mathcal{V}$

We have :

$$Ext^1(\mathbf{1},\mathcal{Y}) \simeq Ext^1(\mathbf{1},\mathcal{V}_1) \times Ext^1(\mathbf{1},\mathcal{W}'_2 \oplus \mathcal{V}') \ \text{ et } Ext^1(\mathbf{1},\mathcal{Y}) \simeq Ext^1(\mathbf{1},\mathcal{V}_2) \times Ext^1(\mathbf{1},\mathcal{W}'_1 \oplus \mathcal{V}').$$

Because $\mathcal{V}_1$ and $\mathcal{V}_2$ are in $\mathbf{V}$, the projection of $\mathcal{U}$ is trivial on $Ext^1(\mathbf{1},\mathcal{W}'_2 \oplus \mathcal{V}')$ and on $Ext^1(\mathbf{1},\mathcal{W}'_1 \oplus \mathcal{V}')$. Then the projection of $\mathcal{U}$ is also trivial on $Ext^1(\mathbf{1},\mathcal{W}'_2 \oplus \mathcal{W}'_1 \oplus \mathcal{V}')$ and thus $\mathcal{W}$ is in $\mathbf{V}$.

Computation of the unipotent radical R_u of the Galois group $G_\mathcal{U}$ of $\mathcal{U}$

By assumption, $\mathcal{U}$ lies in an exact sequence :

$$0 \longrightarrow \mathcal{Y} \overset{i}{\longrightarrow} \mathcal{U} \overset{p}{\longrightarrow} \mathbf{1} \longrightarrow 0 \ .$$

Let R be a C-algebra. Since the categories $< \mathcal{U} >$ and $Rep_{G_\mathcal{U}}$ are equivalent, $\omega(\mathcal{U}) \otimes R$ is an extension of the unit representation $\mathbf{1}_R$ par $\omega(\mathcal{Y}) \otimes R$ in the category $Rep_{G_\mathcal{U}(R)}$ of $G_\mathcal{U}(R)$-modules of finite rank over R. Consider the exact sequence of free R-modules :

$$0 \longrightarrow \omega(\mathcal{Y}) \otimes R \overset{\omega(i)^R}{\longrightarrow} \omega(\mathcal{U}) \otimes R \quad \underset{s^R}{\overset{\omega(p)^R}{\underset{\cdots\cdots}{\rightleftarrows}}} R \longrightarrow 0 \ ,$$

fix a section s of the underlying exact sequence of C-vector spaces, and put $f^R = s^R(1) \in \omega(\mathcal{U}) \otimes R$, where $s^R = s \otimes 1$.

Let us consider the morphism of C-schemes $\zeta_{\omega(\mathcal{U})}^R : G_\mathcal{U}(R) \to \omega(\mathcal{Y}) \otimes R$ defined by the relation :

$$\forall \sigma \in G_\mathcal{U}(R), \zeta_{\omega(\mathcal{U})}^R(\sigma) = (\sigma - 1)f^R.$$

This defines a morphism of schemes $\zeta_{\omega(\mathcal{U})}$ over C from $G_\mathcal{U}$ with value in the C-vector space $\omega(\mathcal{Y})$, whose restriction to R_u is an immersion of algebraic group-schemes over C from R_u to the C-vectorial group $\omega(\mathcal{Y})$. Since $G_\mathcal{U}$ is reduced, its scheme theoretic image is again reduced, and we have :

Lemma 2.2 (see [5], 2.8 and [7], 7.2.3) *The image W of R_u under $\zeta_{\omega(\mathcal{U})}$ is a C-vectorial subgroup of the C vectorial group $\omega(\mathcal{Y})$.*

Proof

Since W is reduced, it suffices to check this on points in the algebraic closure of C. For all $\sigma_1 \in G_{\mathcal{Y}}$ and $\sigma_2 \in R_u$, we have

$$\zeta_{\omega(\mathcal{U})}(\sigma_1 \sigma_2 \sigma_1^{-1}) = \sigma_1(\zeta_{\omega(\mathcal{U})}(\sigma_2)).$$

Indeed, we have :

$$\sigma_1 \zeta_{\omega(\mathcal{U})}(\sigma_1^{-1}) = (1 - \sigma_1)f = -\zeta_{\omega(\mathcal{U})}(\sigma_1), \tag{1}$$

and

$$\zeta_{\omega(\mathcal{U})}(\sigma_1 \sigma_2 \sigma_1^{-1}) = \sigma_1(\zeta_{\omega(\mathcal{U})}(\sigma_2 \sigma_1^{-1})) + \zeta_{\omega(\mathcal{U})}(\sigma_1) = \sigma_1(\sigma_2(\zeta_{\omega(\mathcal{U})}(\sigma_1^{-1})) + \zeta_{\omega(\mathcal{U})}(\sigma_2)) + \zeta_{\omega(\mathcal{U})}(\sigma_1).$$

From (1), we deduce that : $\sigma_1(\sigma_2(\zeta_{\omega(\mathcal{U})}(\sigma_1^{-1}))) = -\sigma_1 \sigma_2 \sigma_1^{-1}(\zeta_{\omega(\mathcal{U})}(\sigma_1))$. But $\sigma_1 \sigma_2 \sigma_1^{-1}$ is an element of R_u and $\zeta_{\omega(\mathcal{U})}(\sigma_1)$ lies in $\omega(\mathcal{Y})$. Then, $\sigma_1(\sigma_2(\zeta_{\omega(\mathcal{U})}(\sigma_1^{-1}))) = -\zeta_{\omega(\mathcal{U})}(\sigma_1)$. Therefore $\sigma_1(\zeta_{\omega(\mathcal{U})}(\sigma_2)) = \zeta_{\omega(\mathcal{U})}(\sigma_1 \sigma_2 \sigma_1^{-1})$ belongs to W.

In other words, W is an algebraic subgroup over C of $\omega(\mathcal{Y})$ which is stable under the action of $G_{\mathcal{Y}}$. Now, $G_{\mathcal{Y}} = \mathbb{G}_m$ and the hypothesis that $\omega(\mathcal{Y})$ is an *isotypic* representation of $\mathbb{G}_m$ implies that W is a C-vectorial subgroup of the C-vectorial group $\omega(\mathcal{Y})$.

Lemma 2.3 (see [5], 2.9) *The image under ω of the smallest sub-object of **V** is equal to W.*

Proof

Let us denote by $\mathcal{V}$ the minimal object of **V**, and by V its image under ω. Then, $G_{\mathcal{U}}$ acts on $\omega(\mathcal{U}/\mathcal{V})$ through $G_{\mathcal{Y}}$ (because $\mathcal{U}/\mathcal{V}$ is a trivial extension of **1** by a quotient of $\mathcal{Y}$ in the category **T**). Thus the projection of $f^C = s(1)$ in $\omega(\mathcal{U})/V$ is invariant under the action of R_u, and the orbit $\{\sigma f^C - f^C ;\ \sigma \in R_u\}$ lies in V. Therefore $\zeta_{\omega(\mathcal{U})}(R_u) := W \subset V$.

Conversely, the image W of R_u under $\zeta_{\omega(\mathcal{U})}$ is, by Lemma 2.2, a C-vector-space stable under the action of $G_{\mathcal{Y}}$ in $\omega(\mathcal{Y})$. Then, by equivalence of category, there exists a sub-object $\mathcal{W}$ of $\mathcal{Y}$ in **T** such that $\omega(\mathcal{W}) = W$. Let us show that $\mathcal{W}$ is an element of **V**. Since W is the image of R_u, $G_{\mathcal{U}}$ acts on $\omega(\mathcal{U})/W$ through its quotient $G_{\mathcal{U}}/R_u = G_{\mathcal{Y}}$. Therefore, $\omega(\mathcal{U})/W(C)$ is an extension of C by $\omega(\mathcal{Y})/W(C)$ in the category $Rep_{G_{\mathcal{Y}}(C)}$. Because $G_{\mathcal{Y}} = \mathbb{G}_m$, this extension is trivial in the category $Rep_{G_{\mathcal{Y}}}$. By the Tannakian equivalence of categories, the extension $\mathcal{U}/\mathcal{W}$ is also trivial in $Ext_{\mathbf{T}}(\mathbf{1}, \mathcal{Y}/\mathcal{W})$, and $\mathcal{W} \in \mathbf{V}$. Then $\mathcal{V} \subset \mathcal{W}$ by minimality. This concludes the proof of Lemma 2.3, hence of Theorem 2.1.

Corollary 2.4 *Let $\mathcal{Y}$ be an object of $\mathbf{T}$, let Δ be the ring $End(\mathcal{Y})$, and let $\mathcal{E}_1, ..., \mathcal{E}_n$ be extensions of $\mathbf{1}$ by $\mathcal{Y}$ such that $\mathcal{E}_1, ..., \mathcal{E}_n$ are Δ-linearly independent in $Ext^1_{\mathbf{T}}(\mathbf{1}, \mathcal{Y})$. Assume that $G_{\mathcal{E}_1}, ..., G_{\mathcal{E}_n}$ are reduced, that $G_{\mathcal{Y}} = \mathbf{G}_m$, and that the action of $\mathbf{G}_m$ on $\omega(\mathcal{Y})$ is given by its canonical character. Then the unipotent radical of $G_{\mathcal{E}_1 \oplus ... \oplus \mathcal{E}_n}$ is isomorphic to $\omega(\mathcal{Y})^n$.*

Proof

For any extension $\mathcal{E}$ of $\mathbf{1}$ by $\mathcal{Y}$, and for any $\alpha \in \Delta$, we denote by $\alpha_*(\mathcal{E})$ the pushout of $\mathcal{E}$ by α ; this is how the structure of Δ-module of $Ext^1_{\mathbf{T}}(\mathbf{1}, \mathcal{Y})$ is defined.

We first note that the direct sum $\mathcal{Y}^n$ admits $G_{\mathcal{Y}^n} = G_{\mathcal{Y}} = \mathbb{G}_m$ as Galois group, and that $\mathbb{G}_m$ again acts on $\omega(\mathcal{Y}^n) = \omega(\mathcal{Y})^n$ through its canonical character. On the other hand, the extension $\mathcal{E}_1 \oplus ... \oplus \mathcal{E}_n$ of $\mathbf{1}^n$ by $\mathcal{Y}^n$ and its pull-back $\mathcal{E} \in Ext^1_{\mathbf{T}}(\mathbf{1}, \mathcal{Y}^n)$ by the diagonal map from $\mathbf{1}$ to $\mathbf{1}^n$ generate in $\mathbf{T}$ the same sub-Tannakian category. Therefore, their Galois groups $G_{\mathcal{E}_1 \oplus ... \oplus \mathcal{E}_n}$ and $G_{\mathcal{E}}$ are equal, and reduced in view of our hypothesis. Let us assume that the unipotent radical R_u of $G_{\mathcal{E}}$ do not fill up $\omega(\mathcal{Y}^n) = \omega(\mathcal{Y})^n$.

By Theorem 2.1, R_u is equal to the C-vectorial group $\omega(\mathcal{V})$ where $\mathcal{V} \in \mathbf{T}$ is the smallest sub-object of $\mathcal{Y}^n$ such that the quotient by $\mathcal{V}$ of the extension $\mathcal{E}$ of $\mathbf{1}$ by $\mathcal{Y}^n$ is trivial in the category $\mathbf{T}$. If $\mathcal{V}$ is not equal to $\mathcal{Y}^n$, then $\omega(\mathcal{V}) \subsetneq \omega(\mathcal{Y}^n)$. Because $\omega(\mathcal{V})$ is a sub-representation of the representation $\omega(\mathcal{Y}^n)$ of $G_{\mathcal{Y}} = \mathbb{G}_m$, it lies in the kernel H of a non trivial $G_{\mathcal{Y}}$-equivariant homomorphism ϕ from $\omega(\mathcal{Y}^n)$ to $\omega(\mathcal{Y})$. By tannakian equivalence of category, there then exists a non trivial morphism $\Phi \in Hom_{\mathbf{T}}(\mathcal{Y}^n, \mathcal{Y})$ such that $\mathcal{V} \subset \mathrm{Ker}(\Phi)$. Now, consider the following diagram :

$$
\begin{array}{ccc}
\mathcal{Y}^n & & \\
\downarrow & \searrow^{\Phi} & \\
\mathcal{Y}^n/\mathcal{V} & \longrightarrow & \mathcal{Y}^n/\mathrm{Ker}(\Phi) \simeq \mathcal{Y}.
\end{array}
$$

Since $\Phi \in Hom_{\mathbf{T}}(\mathcal{Y}^n, \mathcal{Y})$, we can write $\Phi(X_1, ..., X_n) = \alpha_1 X_1 + ... + \alpha_n X_n$, with $\alpha_i \in End_{\mathbf{T}}(\mathcal{Y})$. Then $\Phi_*(\mathcal{E}) = \alpha_{1*}(\mathcal{E}_1) + \alpha_{2*}(\mathcal{E}_2) + ... + \alpha_{n*}(\mathcal{E}_n)$ is a quotient of $\mathcal{E}/\mathcal{V}$, hence a trivial extension of $\mathbf{1}$ by $\mathcal{Y}$ in $\mathbf{T}$. In conclusion, the extension $\alpha_1 \mathcal{E}_1 + ... + \alpha_n \mathcal{E}_n \in Ext^1_{\mathbf{T}}(\mathbf{1}, \mathcal{Y})$ is trivial. But this contradicts the Δ-linearly independence in $Ext^1_{\mathbf{T}}(\mathbf{1}, \mathcal{Y})$ of the extensions $\mathcal{E}_1, ..., \mathcal{E}_n$.

3 Application to Theorem 1.5

We shall apply Corollary 2.4 to the category $\mathbf{T} = \mathcal{T}$ of t-motives, which satisfies $C := End_{\mathcal{T}}(\mathbf{1}) = \mathbb{F}_q(t)$, and all of whose Galois groups are reduced, and to the Carlitz motive $\mathcal{Y} := \mathcal{C}$, for which $\Delta := End_{\mathcal{T}}(\mathcal{C}) = \mathbb{F}_q(t)$ and $G_{\mathcal{C}} = \mathbf{G}_m$ acts on the line $\omega(\mathcal{C})$ through its canonical character. We recall the extensions $X(\alpha_i), i = 1, ..., r$, of $\mathbf{1}$ by $\mathcal{C}$ described in Section 1. Because of Corollary 2.4, the dimension of the algebraic group

$G = G_{\bigoplus_{i=1}^{r} X(\alpha_i)}$ is equal to $1 + n$, where n denotes the dimension of the vector space over $\Delta = \mathbb{F}_q(t)$ generated by the $X(\alpha_i)$'s in $Ext_{\mathcal{T}}^1(\mathbf{1}, \mathcal{C})$.

By an easy computation (similar to [5], 3.8), we get

$$n = max\{s | \nexists f \in \overline{k}(t), (\mu_i)_{i=1}^{s} \in \mathbb{F}_q(t) \text{ not all zero, such that} (t-\theta)f^{(-1)} - f = \sum_{i=1}^{s} \mu_i \alpha_i^{(-1)}(t-\theta)\}.$$

By assumption, $\tilde{\pi}, log_{\mathcal{C}}(\alpha_1), ..., log_{\mathcal{C}}(\alpha_r)$ are linearly independent over $k = \mathbb{F}_q(\theta)$. Following [7], bottom of p. 50, we will now prove that under this hypothesis, n is equal to r.

Suppose that $n < r$. Then, let us consider s such that $\exists f \in \overline{k}(t), (\mu_i)_{i=1}^{s} \in \mathbb{F}_q(t)$ non all equal to zero such that

$$(t - \theta)f^{(-1)} - f = \sum_{i=1}^{s} \mu_i \alpha_i^{(-1)}(t - \theta). \tag{2}$$

It follows from Equation (2) that f is regular at $t = \theta$: if not, $f^{(-1)}$ must have a pole at $t = \theta^{(-1)}$ which implies that f has a pole at $t = \theta^{(-1)}$. By repeating this argument, we get that if f is singular at $t = \theta$ it is also singular at $t = \theta^{(-i)}$ for all $i \geq 1$, which is impossible. Therefore, f and $f^{(-1)}$ are regular at $t = \theta$.

Considering the form of Equation (2), we then get $f(\theta) = 0$. Moreover, the solutions y of (2) are of the following type :

$$y = \mu \frac{1}{\Omega} + \sum_{i=1}^{s} \mu_i L_{\alpha_i}$$

with $\mu \in \mathbb{F}_q(t)$. So, there exists $\mu \in \mathbb{F}_q(t)$, such that :

$$f = \mu \frac{1}{\Omega} + \sum_{i=1}^{s} \mu_i L_{\alpha_i}. \tag{3}$$

By taking $t = \theta$ in (3), we get :

$$0 = \mu(\theta)\tilde{\pi} + \sum_{i=1}^{s} \mu_i(\theta) log_{\mathcal{C}}(\alpha_i).$$

This is a non trivial relation over k between $\tilde{\pi}, log_{\mathcal{C}}(\alpha_1), ..., log_{\mathcal{C}}(\alpha_r)$, which contradicts our assumption.

So, $dimG = r + 1$. This concludes the proof of Theorem 1.5, and implies, as recalled in Section 1, that $trdeg_{\overline{k}}\overline{k}(\tilde{\pi}, log_C(\alpha_1), ..., log_C(\alpha_r)) = r + 1$, i.e. that $\tilde{\pi}, log_C(\alpha_1), ..., log_C(\alpha_r)$ are algebraically independent over $\overline{k}$.

Références

[1] Y. André. Différentielles non commutatives et théorie de Galois différentielle ou aux différences. *Ann. Sci. École Norm. Sup. (4)*,vol. 34, 685–739, 2001.

[2] P. H. Berman and M. F. Singer. Calculating the Galois group of $L_1(L_2(y)) = 0$, L_1, L_2 completely reducible operators. *J. Pure Appl. Algebra*, 139(1-3) :3–23, 1999.

[3] D. Bertrand. Un analogue différentiel de la théorie de Kummer. *Approximations diophantiennes et nombres transcendants* (P. Philippon), W. de Gruyter, 1992, 39-49.

[4] P. Deligne. *Catégories tannakiennes*, volume 87 of *Progr. Math.* Birkhäuser Boston, Boston, MA, 1990, 111-195.

[5] C. Hardouin. Hypertranscendance et groupes de Galois aux différences. arXiv :math.QA/0609646 v2 , Sept. 2006. Submitted for publication, 41 pages.

[6] J.C. Jantzen. Representations of algebraic groups, 2nd edition. *American Mathematical Society*, 2003

[7] M.A. Papanikolas. Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms. arXiv :math.NT/0506078 v1, June 2005. Submitted for publication, 53 pages.

[8] T. A. Springer. *Linear algebraic groups*, volume 9 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, 1998.